[IRIS | Recruitment]

Information Security Assurance Statement [data processors]

Document control	
Version number:	1.3
Owner:	Tom Ross
Date of last update:	November 2025
Document type:	Assurance Statement
Replaces:	1.2
Approved by:	Fran Williams
Approval date:	01/12/2025
Data protection impact screening:	N/A
Date of next formal review:	November 2026

Contents

Information security assurance statement

Objective of this document

The purpose of this information security assurance statement is to provide customers of IRIS | Recruitment by IRIS with transparency as to the security and personal data compliance of this product from all threats, whether internal or external, deliberate or accidental. Also this document aims to ensure legal compliance, business continuity, minimise business damage and maximise client confidence in IRIS | Recruitment as a thoroughly secure software and service provider.

Description of the data processing carried out by IRIS | Recruitment

- Capture and storage and processing of recruitment activity information including:
    - Employee details
    - Authorisation process
    - Planned, live and historic information about vacancies
    - Candidate information
    - Application information, including special category data

Statement of assurance

IRIS | Recruitment will ensure that:

1. We will put in place measures to protect customer information from a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;
2. We will meet our regulatory and legislative requirements.
3. We will produce, maintain and test Business continuity plans.
4. We will provide information security training to all our staff
5. We will report and investigate information incidents (whether actual or suspected), in line with our Incident reporting procedure.
6. We will monitor compliance with our Information Security Policy.

IRIS ensures that all employees comply with corporate standards and procedures. These include incident handling, information backup, system access, virus controls, passwords-authentication, communication and encryption. These policies are communicated to all employees via the company compliance portal and intranet.

IRIS | Recruitment Organisational Security

IRIS | Recruitment is part of the IRIS Software Group.

Organisational security at IRIS Group level

Data protection and information security at IRIS Software Group is controlled by the *IRIS Privacy, Security and Compliance Steering Group*. This group meets at least quarterly and includes:

- Members of the Executive Committee

- The Chief information Officer (CIO)
- IRIS Group IT Director
- IRIS Group Data Protection Officer
- IRIS Group Compliance Manager
- Other key security leads within the company

The Privacy, Security and Compliance Steering Group approves IRIS Group level policies relating to information security and data protection, which IRIS products must comply with. There are three Group policies and a detailed Information Security Management System (ISMS). The three Group level policies are:

- IRIS Group Data Protection Policy – this sets out the roles and responsibilities for data protection compliance within the IRIS Group. It also sets out the requirement for risk assessment and data protection assessment for all projects and proposals that will change or impact on the handling or use of personal data.

- Information Security and Acceptable Use Policy Summary – this sets out the basic information security and acceptable use standards that all staff within the IRIS Group are required to adhere to.

- IRIS Personal data incident reporting and investigation procedure – this indicates the reporting and investigation procedure for all security incidents that become known or are reported to anyone within the IRIS Software Group.

The above policies are communicated to all staff and relevant external staff within the IRIS Group at least annually, using a dedicated training and policy management platform. Managers responsible for delivering IRIS products and services are required to ensure local arrangements are in place to comply with those policies and to evidence this.

- IRIS ISMS – This is the default security system for IRIS Software Group. All IRIS products must meet or be working towards meeting the standards of the IRIS ISMS except for those which already have their own certification under ISO27001 or any other standard relating to information security and data protection.

Organisational security for IRIS | Recruitment

At IRIS | Recruitment, the product manager is the single point of contact for routine security and data protection enquiries. They work with the managers involved in delivering IRIS | Recruitment to ensure IRIS | Recruitment complies with the IRIS Group policies and ISMS or any other information security standard – as well as any other regulatory requirements relevant to the service.

For IRIS | Recruitment, the team with responsibility for ensuring your data remains secure and in compliance with IRIS Group Policies and ISMS are:

- Fran Williams, Senior Director, Product
- Tom Ross, Product Manager
- Chris Malcolm – Director, Engineering
- Chris Renton, Software Engineering Manager
- Olivia Bradshaw, Implementation Manager (Laura Cundall (Maternity Cover))
- Tim Johnstone, Director, DevOps
- Thomas Derbyshire, Senior Manager, Customer Services

The IRIS | Recruitment team keep your data secure by ensuring that appropriate measures are implemented to protect your data from accidental or unlawful destruction, loss, alteration, unauthorised

disclosure of, or access to your data while being stored, transmitted or otherwise processed by or on behalf of IRIS | Recruitment.

Measures are “appropriate” if they have been identified through risk assessment.
Date of last IRIS | Recruitment risk assessment review: 24/11/25

The IRIS | Recruitment team will ensure adequate records are created and maintained to support compliance verification and inspections and incident response (subject to any limitations set out in our Terms and Conditions).

The IRIS Group Data Protection officer is responsible for providing advice and guidance to the IRIS | Recruitment team and for monitoring our compliance on all security policies and related issues. The IRIS Group Data Protection Officer is also the designated contact for the Information Commissioner’s Office.

The IRIS DevOps team are responsible for the operation and integrity of IRIS | Recruitment’s IT systems and for keeping systems up to date.

IRIS | Recruitment’s development systems are managed by the IRIS IT Department.

Asset register: IRIS Group IT records and maintains a register of all assets, relevant to IRIS | Recruitment (including acquired software licences) in a fixed assets system.

Client defined classifications: Client information and materials processed, stored or transmitted by IRIS | Recruitment shall be handled strictly in line with the customer’s prior advised classification policies and standards, subject only to legal compliance

IRIS | Recruitment human resource security

Some IRIS | Recruitment staff will have access to your data.

Prior to employment

- Staff and contractors are subject to background checks and verifiable references to ensure suitability for any given job role.

- All staff are required to accept our Group Data Protection Policy, Incident Reporting Procedure and Information Security & Acceptable Use Policy.

During employment

- Access is granted following the principle of least privilege. By default, employees have no access and are only granted access to data where their job function requires it.

- As part of regular security awareness training, IRIS | Recruitment managers are made aware of their responsibilities to ensure that established policies and procedures are adhered to by external parties, contractors and employees.

- IRIS | Recruitment employees, third parties and contractors receive appropriate awareness training and regular updates in organisational policies and procedures as relevant for their job function. Corporate policies and training are administered via MetaCompliance and KnowBe4.

- A formal and communicated disciplinary process is implemented to handle IRIS | Recruitment employees who have committed a security breach.

Termination and change of employment

- There is a formal procedure for performing employment terminations and change of employment. This procedure includes information on responsibilities for the following actions:
    - Ensuring the employee is aware of the need to maintain confidentiality after employment ceases
    - Restricting the person's access to confidential areas immediately
    - Full removal of access to any part of the corporate network prior to departure,
    - All corporate assets in that person's possession having been returned
    - In the event of a person transferring from one department to another within IRIS Software Group that person's access will be varied accordingly.

IRIS | Recruitment Access Control

Access is granted following the principle of least privilege. By default, employees have no access and are only granted access to data where their job function requires it.

The default password rules are:

- Password must be at least 8 characters
- The password must contain letters, upper- and lower-case characters, at least one number, at least one 'special' character.

Clients can amend their own password rules, and can include:

- Password length
- If passwords must contain letters, upper- and lower-case characters, at least one number, at least one 'special' character.
- Password expiry
- Allow / Force 2FA
- Number of attempts before account lock-out
- Account lock-out duration
- Restrict access to SSO only. This is useful for clients who need to centralise their account management processes.

These rules are enforced through the Recruitment ATS.

Most access controls can be amended by the clients directly, but where help is needed the IRIS | Recruitment help desk will assist. To request help one of the identified primary users must raise a ticket to ensure there is an audit trail of these changes. This audit is retained for the life of the contract with the client.

Within IRIS there are also the following additional controls:

- **User registration and de-registration** – A formal documented registration and de-registration procedure.
- **User access provisioning** – There is a documented procedure for approving and setting up user access in accordance with access control policies. This is based on job role requirements
- **Management of privileged access rights** - Privileges are allocated on need-to-use basis; privileges are allocated only after formal authorisation process.
- **Management of secret authentication information of users** - The allocation and reallocation of secret authentication information - e.g. passwords should be controlled through a formal management process. Users are asked to sign a statement to keep this information confidential.

- **Review of user access rights** - Admin user accounts are reviewed quarterly.
- **Removal or adjustment of access rights** - For internal staff / admin users, access is via SSO only and is therefore disabled immediately upon termination.
- **Use of privileged utility programs** - N/A
- **Access to program source code** - Only authorised developers have access, using secure version control (via Azure DevOps). All changes require peer review and automated checks before release. Restricted access controls are in place to prevent unauthorised code changes and to protect information.

For the avoidance of doubt, IRIS | Recruitment warrants to Clients that it will not seek to circumvent, compromise or change the Client's security controls, and IRIS | Recruitment will not change the Client's software configurations (without proper authorisation); and no 'back door' password or other method of remote access into IRIS | Recruitment's software shall exist.

Encryption (cryptology)

In transit

All information to and from the system is encrypted in transit using TLS1.2 with a SHA256 SSL certificate.

At rest

We encrypt sensitive data such as passwords using HMAC SHA2-512 encryption. Additional information captured from the candidates can be set to be encrypted at rest as required.

IRIS | Recruitment physical and environmental security

Our hosting provider, Rackspace, has industry leading physical security procedures and measures in place to protect personal data.

Rackspace Technology is a leading provider of expertise and managed services across all the major public and private cloud technologies.
The data centre used for IRIS Recruitment is located in the UK.

Equipment

All equipment used for the provision of the IRIS | Recruitment ATS is hosted and managed by trusted third-party providers, primarily Rackspace and Microsoft Azure. Both providers maintain industry-leading physical and environmental security controls, with certified data centre standards, to ensure the protection of personal data and the resilience of services.

IRIS operates a clear desk policy with automated screen locking and password protected screen savers forced via group policies.

Media handling

USB storage devices are disabled, and the principle of least privilege is applied to all user accounts. User accounts are regularly reviewed.

Data is never downloaded from the ATS and transferred via Physical Media by any employee of IRIS.

Operations security

Documented operating procedures

There are documented operating procedures to support operational activities associated with information processing and communication facilities; backup processes, transmission of confidential information, equipment maintenance, etc

Change management

Change management controls have been implemented to ensure satisfactory control of all changes.

Capacity management

The use of resources are monitored, tuned and protections are made of future capacity requirements to ensure systems continue to perform at optimum levels.

Separation of development, testing and operational environments

The development and testing facilities are isolated from operational facilities; development software runs on a different environment to the production software.

Protection from malware

IRIS | Recruitment utilises virus and malware protection to protect against malicious software and this is centrally monitored. All servers are automatically updated. Firewalls are in place.

For emails, Mimecast is used to provide comprehensive email filtering (not only to preclude spam but also to scan attachments more effectively to counteract viruses and other malware).

Back-ups

Back-ups of the database are performed weekly. These backups are retained for 2 weeks.

Event logging

All servers are configured to log user activities, exceptions, faults and information security events.

Protection of log information

Security controls are in place to prevent tampering of the log information and audit trails.

Administrator and operator logs

System administrator and system operator activities are logged, and the logs protected and regularly reviewed

Clock synchronisation

IRIS Group IT controls clock settings, ensuring that synchronisation is enabled to a real time clock set at local standard time

Control of operational software

Controls are in place for the implementation of software on operational systems to minimise the risk of corruption of operational systems.

Management of technical vulnerabilities

Automated penetration tests are performed on a monthly basis. Independent penetration tests are commissioned annually.

Restrictions on software installations

Rules for governing the installation of software by users have been established and implemented.

Communications security

Network controls

Controls are in place to ensure the security of information in networks and the protection of connected services from unauthorised access

Segregation of networks

Development, Testing and Product environments are segregated to facilitate effective information security.

Electronic messaging

IRIS | Recruitment has a policy in place for the acceptable use of email, instant messaging and other electronic communications

Confidentiality or non-disclosure agreements

The requirements for confidentiality or non-disclosure have been identified, reviewed, documented and reflect the product's needs for the protection of information

Information transfer policies and procedures

Policies are in place to protect the transfer of information.

IRIS | Recruitment staff are reminded to maintain the confidentiality of sensitive information while using technology such as email, phones, fax and voicemail via these procedures, which must be reviewed by each individual annually.

Agreements on information transfer

External suppliers are reviewed annually to ensure there are adequate controls in place to ensure the secure transfer of business information between IRIS | Recruitment and external parties.

System acquisition, development and maintenance

Information security requirements analysis and specification

Any new system is evaluated and adequate security requirements are derived from business requirements, relevant legal and regulatory acts, internal policies and any other source that may have an impact on confidentiality, integrity or availability of information assets at IRIS | Recruitment.

For internal systems and client facing applications the Product Team document the security requirements.

The minimum security requirements are that the new or revised system does not introduce any new security risks and is compatible with the current IRIS | Recruitment risk appetite.

Risk assessments are conducted or reviewed on regular intervals or when there is a significant change in business to ensure that any new system specification is conformant with the above.

Security in development and support processes

Secure development policy

Security has been integrated in all phases of software development and documented in a secure development policy

System change control procedures

There is a formal change control process that ensures that that major system changes are controlled.

Technical review of applications after operating platform changes

There is a formal change control process that ensures that that application systems are reviewed and tested after changes to the operating system / infrastructure.

Restrictions on changes to software packages

All changes to the software go through a formal change control process.

Secure system engineering principles

Principles and procedures for engineering secure systems have been established, documented, maintained and applied to all information system implementation efforts

Secure development environment

Risk assessments have been performed on the entire system development lifecycle. Specific Data Protection Impact Assessments are performed for feature developments.

System security testing

Automated and manual testing is included in software development projects including test inputs and expected outputs under a range of conditions.

System acceptance testing

Acceptance testing is performed before any new release.

Test data

Protection of test data

The test environment is separate from the production environment to ensure confidential and personal information is never used for test purposes.

Processing locations and international data transfers

On occasion, IRIS may use engineers and third parties located in India for production environment support, deployment activities, access management and security & vulnerability management. In all these instances, information is held on secured network drives held in the UK and only accessible by those authorised to process it.

All relevant security requirements have been addressed and further information is available on request. A full risk assessment is carried out annually to ensure that client data is always protected.

Supplementary measures for personal data processed in India

IRIS and its engineers in India adhere to the standards of ISO 27001 and uses privileged access management controls to audit activity of engineers. VPNs and Bastions are used where appropriate and all communications are over encrypted channels. IRIS has an international data transfer agreement in place with all sub-processors used that are based in India. This requires them to comply with IRIS data protection and security policies and standards, particularly in relation to handling requests from official sources.

Supplier relationships

Information security policy for supplier relationships

All supplier relationships are subject to a risk assessment prior to any exchange or delivery of information assets.

IRIS | Recruitment takes the following into account when considering and conducting supplier agreements:

- The business case for supply chain security
- Information risk within the supply chain, and associated threats
- The nature of the relationship – acquisition or supply of information assets
- Organisational capability of assuring information security, with regard to both IRIS | Recruitment and the supplier
- System lifecycle processes for the assurance of information security
- ISMS processes and controls in relation to system lifecycle processes
- ISMS processes and controls in relation to security of the supply chain
- Essential security practices within the supply chain

The risk assessment will identify controls required to address risk associated with the provision of the service.

Addressing security within supplier agreements

IRIS | Recruitment carries out a risk assessment to identify risks related to external party access and select controls to mitigate any identified risks.

IRIS | Recruitment implements those controls that are within its own power.

IRIS | Recruitment agrees with the external party those controls that the external party is required to implement and documents them in an agreement (drawn up by IRIS's legal advisers) that the third party signs.

Where the required controls are within the scope of a recognised standard or scheme (e.g. IEC/ISO 27001), the organisation may choose to select providers based on their ability to demonstrate accredited certification (or a similar level of assurance) to the requirements of the standard or scheme provided that the scope of certification includes the services organisation wishes to procure.

The agreements between IRIS | Recruitment and external parties are created by IRIS's legal advisers.

Information and communication technology supply chain

Agreements with suppliers include requirements to address the information security risks associated with information and communications technology services and product supply chain.

Monitoring and review of supplier services

The external party agreement includes reporting structures, defines acceptable levels of performance and provides monitoring, inspection and audit rights. Supplier reviews are performed annually.

The relationship owner monitors performance against the service and security criteria contained in the agreement, ensures that reports required under the agreement are delivered as required and reviews them, and conducts regular progress meetings as required.

The relationship owner ensures that information security incidents experienced by the third party are reviewed jointly and that relevant information security incidents experienced internally are communicated to the third party to that appropriate steps can be taken.

The relationship owner identifies any problems of any sort on either side of the relationship, and ensures that they are resolved, using the agreed escalation procedure where necessary.

The Product Manager is responsible for reviewing the third party's internal audit trails and records of security events.

Where a supplier has been selected on the basis of its compliance with an information security scheme or standard, the results of independent third-party audit will be deemed as evidence that information security controls are in place and operating effectively.

On a regular basis, the Product Manager reviews all outstanding actions in respect of deficiencies in third-party services to ensure that appropriate corrective or preventive action is being taken, having regard to the fact that ultimate responsibility for the information processed by the third party remains with IRIS | Recruitment.

Managing changes to supplier services

IRIS | Recruitment may need to agree changes to external party contracts and agreements to take account of changes that it makes to, or as a result of:

- The services it currently offers to its clients
- New applications and systems it has developed or acquired
- Modifications, changes or updates to its own policies and procedures
- New or amended controls arising from new risk assessments or information security incidents

The external party may need to request changes to the contract in order to implement:

- Changes or improvements to their networks or other infrastructure
- New or improved technologies, new products or new releases of current products
- New development tools, methodologies and environments
- New physical locations or physical services
- New vendors or other suppliers of hardware, software or services

Any changes that may be required are subject to a new risk assessment (taking into account the criticality of the business systems involved) and review of the selected controls.

New controls, or changes to existing controls are identified, authorised, agreed with the third party, and made the subject of an agreed variation to the existing contract.

The relationship owner is responsible for ensuring that the revised controls are implemented and incorporated into the existing review and monitoring arrangements.

Summary of sub-processors

Provider	Purpose	Description	Data Location
Rackspace	Hosting	Rackspace host the application and database	UK
Microsoft Azure Hosting	Hosting	Microsoft Azure Hosting hosts some elements of the application and database, and project in 2025 / 2026 planned to migrate hosting to Azure	UK
Microsoft Azure DevOps	SDLC	Development lifecycle is managed on Microsoft Azure Dev Ops, with 4th Line Support Tickets managed via the support & development functions on the platform	UK
Amazon Web Services	Automation and comms	AWS technologies are leveraged to provide automations and enhancements to customer services – including query resolution/management/communications	UK & US
Intercom, Inc.	AI-driven customer service and messaging platform	Intercom technologies are leveraged to provide automations and enhancements to customer services – including query resolution / management / communications.	UK & US
Reach Interactive	SMS Sending	Content of SMS messages, recipient mobile phone number	UK

SendGrid	Email Sending	Content of Emails, sent from email addresses, recipient email addresses	USA
Brevo (SendInBlue)	Email Sending	Content of Emails, sent from email addresses, recipient email addresses	France
Gainsight	Product analytics platform	Provides customer health scoring, analytics, and insights to support user engagement	EU
Sales Cloud via Salesforce	Support	Our support function uses Sales Cloud to provide customer ticketing, communication, live chat and query resolution management.	UK
Cybage PTY Limited	SDLC	3rd party software development partner who support us with DevOps processes for IRIS Recruitment.	India

Additional sub-processors may be used for additional modules. These will be detailed with the module information.

Information security incident management

Responsibilities and procedures

The IRIS DPO is responsible for the Information Security Incident Management Procedure.

Users and owners of organisational information security assets are required to follow the Information Security Incident Management Procedure for reporting information security weaknesses or events, and this is documented in the Acceptable Use Policy.

The IRIS DPO is responsible for logging and following up on reported incidents and weaknesses.

Information security events and weaknesses are reported to the IRIS DPO in line with the documented procedure.

The IRIS DPO is responsible for user training and awareness and for selecting those events which can be used to support training activities.

The IRIS DPO will oversee communication with relevant parties regarding a data breach, including the client(s) involved, the data subject(s) affected and the ICO.

Reporting information security events

IRIS has a standard group wide Incident Reporting Procedure to report security incidents through the management channels as quickly as possible.

Reporting information security weaknesses

IRIS has a standard group wide formal reporting procedure for users to report security weakness in, or threats to, systems or services.

Assessment of and decision on information security events

IRIS has a documented Incident Response Plan which details assessing information security problems and issues and classifying them as information security incidents that need to be reported through the corporate procedure.

Response to information security incidents

There are documented procedures in place for responding to an information security incident.

Any requests from customers for assistance via our help desk with suspected breaches with be prioritised to the highest level and forwarded to the IRIS DPO.

Learning from Incidents

The Incident Response Plan details the activities that must take plan during the Post Incident Review.

This step contains the impact of the incident, actions taken, training gaps, incident timeline, notes taken and any odd information that arose during the process of the incident. This document often reveals an underlying issue that is the root cause of the incident. This is crucial for healthy growth following an incident.

Collection of Evidence

All information gathered during the course of responding to an Information Security Incident is potentially evidence to be used in a disciplinary, criminal or civil action.
Care is taken to preserve the evidence in such circumstances.

Business continuity – Information security aspects

Planning information security continuity

IRIS | Recruitment has determined its requirements for information security and the continuity of information security management in adverse situations and these are documented in the Business Continuity Plan.

Implementing information security continuity

IRIS | Recruitment has documented processes, procedures and controls that are regularly maintained and implemented to ensure an appropriate level of business continuity during an adverse situation

Verify, review and evaluate information security continuity

Information security continuity controls are reviewed at regular intervals to ensure that they are valid and effective during adverse situations, these reviews are performed at least annually.

Availability of information processing facilities

The Business Continuity Plan addresses all the information continuity components of IRIS | Recruitment's activities and ensures that adequately trained resources are available to provide continuity of all the identified information security assets, including taking appropriate steps for the protection of employees (including information processing employees) and all information processing facilities.

Compliance

Identification of legislation and contractual requirements applicable to IRIS | Recruitment

All relevant statutory, regulatory and contractual requirements have been explicitly defined and documented for the information systems involved in IRIS | Recruitment. Specific controls and individual responsibilities at product level have been defined and documented to meet these requirements.

Intellectual Property Rights (IPR)

IRIS has group wide procedures to ensure compliance with legal restrictions on use of material in respect of which there may be intellectual property rights such as copyright, design rights, trademarks.

Protection of records

Important records of the organisation are protected from loss, destruction, falsification unauthorised access and unauthorised release.

Privacy and protection of personally identifiable information

IRIS has a group wide Data Protection Policy and controls in place to protect the privacy of personal information in accordance with legislation and regulation.

Regulation of Cryptographic Controls

IRIS have a group wide Encryption policy which details when cryptographic controls should be used, how they should be used, and the management of encryption keys.

Information security reviews

Independent review of information security

IRIS policies and procedures are independently audited annually as per the requirements of the ISO 27001 and ISO 9001.

Compliance with security policies and standards

Internal audits are conducted to test all aspects of the IRIS Information Security Management System.

Technical compliance review

Automated penetration tests are performed regularly on the IRIS | Recruitment solution. Independent penetration tests are commissioned annually.

Data Protection – quick reference

IRIS Group Data Protection Officer

Vincenzo Ardilio (dataprotection@iris.co.uk)

Data protection owner for IRIS | Recruitment

Tom Ross (tom.ross@iris.co.uk)

Categories of personal data processed as part of IRIS | Recruitment

IRIS | Recruitment will capture a large amount of Personally Identifiable Information about candidates during the application process.

What is captured is defined by clients and may include the following:

- Name
- Address
- Contact details
- Race
- Ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Health data
- Sex life
- Sexual orientation

Categories of data subjects under the product/service provision

- Employees
- Candidates

Location of personal data processing, hosting and access by IRIS agents

All data is stored in the UK.

On occasion, IRIS may use engineers and third parties located in India for production environment support, deployment activities, access management, and security and vulnerability management.

In all these instances, information is held on secured network drives held in the UK and only accessible by those authorised to process it.

All relevant security requirements have been addressed and further information is available on request.

A full risk assessment is carried out annually to ensure that client data is always protected.

Retention of data

There are settings within the IRIS | Recruitment ATS to allow clients to define their own retention periods for the various types of data. By default, these are all set to 24 months.

On the termination of a client's contract, select data will be provided to clients and then the data will be removed from the IRIS | Recruitment servers.

Customers can manually delete data within the system themselves.

Data subject rights

The right of access

Candidates can access all their data via their candidate account.

If a candidate chooses to submit a Subject Access Request, there is a Subject Access Request feature within IRIS | Recruitment which will extract all the information help about that candidate, allow redaction where required and send the information to the candidate. This process is fully audited.

The right to rectification

Candidates can update their candidate information at any time, they can update their application information up until the application is submitted.

Candidates can view the information they have submitted and request a change to the client.

The right to erasure

Candidates can submit erasure requests to client. There are tools within IRIS | Recruitment to action erasure requests. This process is fully audited.

The right to restrict processing

Within the candidate account the candidate can perform the following at any time:

- Withdraw their application
- Remove themselves from searches
- Deactivate their account

The right to data portability

From within the candidate account, the candidates can download a copy of all their data in electronic format (XML).

The right to object

Any automated decisions made during the application process are highlighted to candidates from within their candidate account, along with a link allowing them to request manual intervention.

GDPR Principles

IRIS | Recruitment stores 3 types of personal information covered by the GDPR; Candidate account information, application information and employee information.

Within the GDPR there are seven key principles. These are listed below along with how IRIS | Recruitment adheres to those principles.

Lawfulness, fairness and transparency

Candidate Account Information	**Consent** When a candidate creates an account, they are presented with a privacy policy containing details of the purpose of storing the data, who it will be shared with and how long it will be retailed. For our clients, for whom we are the data processor, this privacy policy can be customised by them as the data controller.
Application Information	**Contract** When a candidate applies for a role, they are presented with a privacy policy specific to that role containing details of the purpose of storing the data, who it will be shared with and how long it will be retailed. For our clients, for whom we are the data processor, this privacy policy can be customised by them as the data controller.
Employee HR Information	**Legitimate Interest** Employees are informed what information is stored about them and what it is used for when they are initially employed.

Purpose limitation

The data IRIS | Recruitment store will only be used for the purposes it was originally captured.

For our clients, for whom we are the data processor, it is their responsibility to ensure they only use the candidate and application data for the purposes it was originally captured.

Data minimisation

IRIS | Recruitment will only request the information required for the purpose it is being captured for and no more.

For our clients, for whom we are the data processor, it is their responsibility to ensure they are requesting only the information required during the application process.

Accuracy

Candidate Account Information	The date the information was last updated is stored.
Application Information	The date the information was submitted is stored.
Employee HR Information	Employee details are verified regularly as appropriate.

Storage limitation

Candidate Account	Data is automatically purged after a given period Data Protection Policy (Public) v1.3 Page 6 Information controlled by settings in the recruitment system, for IRIS | Recruitment this is set to 24 months. For our clients, for whom we are the data processor, the data purge settings are defined by them as the data controller.

Application Information	Data is automatically purged after a given period controlled by settings in the recruitment system, for IRIS | Recruitment this is set to 24 months. For our clients, for whom we are the data processor, the data purge settings are defined by them as the data controller.
Employee HR Information	Employee details are retained for a period of 6 years after the employment has been terminated, to cover the time limit for an individual to be able to bring any civil legal action.

Integrity and confidentiality

All IRIS | Recruitment systems are written with Privacy by Design. The development team follows documented secure development practices, and the systems are regularly penetration tested by independent parties to ensure the systems remain as secure as possible.

IRIS employees are trained annually on Information Security.

Accountability

IRIS takes their responsibility to ensure compliance with the GDPR very seriously. IRIS has employees who are certified GDPR Practitioners and have assigned a Data Protection Officer. All IRIS employees are trained annually on information security.